



NIT-407

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

A. SHIMIZU et al.

Confirmation No. 7747

Serial No. 10/759,204

Group Art Unit: 2181

Filed: January 20, 2004

Examiner: R. Borkowski

For: COMPUTER SYSTEM CONTROLLING ACCESSES TO STORAGE
APPARATUS

Customer No.: 24956

SUBMISSION OF CERTIFIED PRIORITY DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

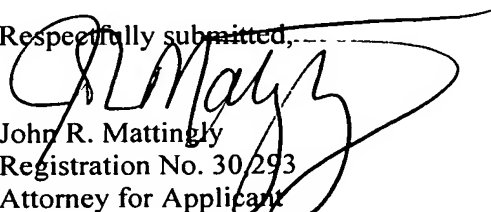
Sir:

Applicants submit herewith a certified priority document of the corresponding
Japanese Patent Application:

No. 2003-093140, filed March 31, 2003, for the purpose of claiming foreign priority
under 35 U.S.C. § 119.

Applicants respectfully request that the priority document be submitted and officially
considered of record.

Respectfully submitted,


John R. Mattingly
Registration No. 30,293
Attorney for Applicant

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 Diagonal Road, Suite 370
Alexandria, Virginia 22314
(703) 684-1120
Date: May 10, 2006

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出 願 年 月 日 2 0 0 3 年 3 月 3 1 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 0 9 3 1 4 0
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 0 9 3 1 4 0]

願 人 株式会社日立製作所
Applicant(s):

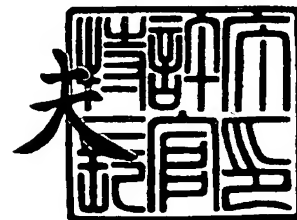
CERTIFIED COPY OF
PRIORITY DOCUMENT

NIT-407

2 0 0 4 年 1 月 2 3 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



BEST AVAILABLE COPY

出証番号 出証特 2 0 0 4 - 3 0 0 2 0 3 1

【書類名】 特許願

【整理番号】 H03000941A

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 12/00

【発明者】

 【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地 株式会社日立製作所中央研究所内

 【氏名】 清水 晃

【発明者】

 【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地 株式会社日立製作所中央研究所内

 【氏名】 藤原 真二

【特許出願人】

 【識別番号】 000005108

 【氏名又は名称】 株式会社 日立製作所

【代理人】

 【識別番号】 100075096

 【弁理士】

 【氏名又は名称】 作田 康夫

 【電話番号】 03-3212-1111

【手数料の表示】

 【予納台帳番号】 013088

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ストレージ装置でアクセス制御を行う計算機システム

【特許請求の範囲】

【請求項 1】

計算機システム上で動作するプログラムの実行によりストレージに対する I/O 要求を発行する I/O 要求方法であって、前記プログラムに予め設定されたプログラム識別子と要求アドレスを、2つの値を入力として1つの値を生成する第1の関数に適用して識別子付アドレスを生成し、該識別子アドレスを用いて I/O 要求を発行することを特徴とするストレージ装置への I/O 要求方法。

【請求項 2】

ストレージに対する I/O 要求を発する第1のプログラムと、該 I/O 要求を取りまとめ I/O コマンドをストレージ装置に対して送信する第2のプログラムが動作する計算機において、

前記第1のプログラムは予め設定されたプログラム識別子と要求アドレスを、2つの値を入力として1つの値を生成する第1の関数に適用して識別子付アドレスを生成し、該識別子アドレスを用いて I/O 要求を発行し、

前記第2のプログラムは、プログラム識別子と論理ボリュームとネットワークアドレスの対応表を保持し、

保護指定された論理ボリュームへの I/O 要求の場合、1つの値を入力とし2つの値を生成する前記第1の関数に対応する第2の関数により、前記 I/O 要求の識別子付アドレスから元の要求アドレスとプログラム識別子を取り出し、該対応表よりプログラム識別子と論理ボリュームから対応するネットワークアドレスを検索し、該ネットワークアドレスを送信元としてストレージ装置と通信を行い、前記元の要求アドレスに対する I/O コマンドを送信することを特徴とする計算機。

【請求項 3】

1つ以上の計算機と1つ以上のストレージ装置がネットワーク装置により接続されている計算機システムにおいて、

前記計算機は、

ストレージに対する I/O 要求を発する第1のプログラムと、該 I/O 要求を取り

まとめ I O コマンドを送信する第 2 のプログラムが動作し、該第 1 のプログラムは予め設定されたプログラム識別子と要求アドレスを、2 つの値を入力として 1 つの値を生成する第 1 の関数に適用して識別子付アドレスを生成し、該識別子アドレスを用いて I O 要求を発行し、該第 2 のプログラムは、プログラム識別子と論理ボリュームとネットワークアドレスの対応表を保持し、保護指定された論理ボリュームへの I O 要求の場合、1 つの値を入力とし 2 つの値を生成する前記第 1 の関数に対応する第 2 の関数により、前記 I O 要求の識別子付アドレスから元の要求アドレスとプログラム識別子を取り出し、該対応表よりプログラム識別子と論理ボリュームから対応するネットワークアドレスを検索し、該ネットワークアドレスを送信元としてストレージ装置と通信を行い、前記元の要求アドレスに対する I O コマンドを送信するものであり、

前記ネットワーク装置は送信元ネットワークアドレスによりストレージ装置への通信の可否を判断することを特徴とする計算機システム。

【請求項 4】

請求項 3 の計算機システムにおいて、前記ネットワーク装置に替えて前記ストレージ装置で論理ボリュームへのアクセス可否を判断することを特徴とする計算機システム。

【請求項 5】

論理ボリューム識別子と該論理ボリュームへのアクセスを許可するプログラム識別子の対応表を保持し、

受け付けた I O コマンドより保護指定された論理ボリュームに対する I O コマンドを選び、

1 つの値を入力とし 2 つの値を生成する第 2 の関数により該 I O コマンドのアドレスから第 2 のアドレスとプログラム識別子を取り出し、

該プログラム識別子と該対応表より該論理ボリュームへのアクセスの許可を判断し、

アクセスが許可された該 I O コマンドのアドレスを第 2 のアドレスに修正して I O コマンドを処理することを特徴とするストレージ装置のアクセス制御方法。

【請求項 6】

ストレージ装置識別子と論理ボリューム識別子と該ストレージ装置に対して転送を許可するプログラム識別子の対応表を保持し、

ネットワークを流れるパケット内にある I O コマンドから保護指定されたストレージ装置の論理ボリュームに対する I O コマンドを選び、

1 つの値を入力とし 2 つの値を生成する第 2 の関数により、該 I O コマンドのアドレスから第 2 のアドレスとプログラム識別子を取り出し、

該プログラム識別子と該対応表より該パケットの転送の許可を判断し、

アクセスが許可された該 I O コマンドのアドレスを第 2 のアドレスに修正してパケットを流すことを特徴とするネットワーク装置におけるアクセス制御方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、プログラム、ネットワーク装置、ストレージ装置、およびそれらを用いた計算機システムに関係するもので、特に高いセキュリティが要求されるものに関係する。

【0 0 0 2】

【従来の技術】

計算機に直接接続されているストレージ装置では通常はアクセス制御を行っておらず、直接接続された計算機から発行された I O コマンドは無条件に処理されている。また、1 つ以上のストレージ装置を 1 つ以上の計算機で共有する S A N (S t o r a g e A r e a N e t w o r k) では、ゾーン設定などによる計算機単位でのアクセス制御を行っているが、アクセスが許可された計算機からの I O コマンドは無条件に処理される。

この様に、ストレージ装置ではアクセスが許可された計算機からの I O コマンドは無条件に処理されるため、計算機が不正使用された場合、ストレージ装置に格納されているデータは盗み見られ、最悪の場合には改竄される虞れもある。計算機が不正使用されないための対策は数多く存在するが、必ずしも完全ではない。盗み見られても解読できないようにデータを暗号化する対策もあるが、暗号が解読された場合は盗み見られてしまう。

【0003】

計算機が不正使用された場合も、なおデータが盗み見されたり改竄されたりするのを防ぐためには、計算機上のアクセス制御とは別に、ストレージ装置におけるアクセス制御を行うのが有効である。特に、特開 2 0 0 2 - 2 2 2 1 1 0 号公報（特許文献 1）に開示された方法では、ストレージへアクセスするアプリケーションプログラムを単位としてストレージ装置のアクセス制御を行う。したがって、ユーザもしくは計算機管理者が悪用された場合にもデータのセキュリティを保つことが可能となる。しかしながら、上記特許文献 1 のアクセス制御を実現するには特殊な OS が必要であり、また計算機とストレージ装置間のプロトコルを拡張する必要がある。

【特許文献 1】

特開 2 0 0 2 - 2 2 2 1 1 0 号公報

【0004】**【発明が解決しようとする課題】**

したがって本発明においては、計算機が不正使用された場合にプログラムが管理するデータが盗み見られ、データが改竄／消去されてしまう問題を解決する。さらに、各種プロトコルを変更せず、特定の計算機や OS を前提としないアクセス制御方法を提供する。

【0005】**【課題を解決するための手段】**

上記課題を解決するために、ストレージ装置またはネットワーク装置においてプログラム単位でアクセス制御をおこなう。プログラム単位でアクセス制御を行うために、プログラムにプログラム識別子を設定し、IO コマンドと共にストレージ装置またはネットワーク装置にプログラム識別子を渡す。ストレージ装置およびネットワーク装置では上記プログラム識別子により IO コマンドの実行可否を決める。プロトコルを変更せずにプログラム識別子を渡すために、IO 要求や IO コマンドに含まれる特定の値にプログラム識別子を埋め込む。つまり、2 つの値 x 、 y からある値 z を生成する関数 $f(x, y)$ と、その逆である z から 2 つの値 x 、 y を取り出す逆関数 $g(z)$ を決める。IO 要求を発行するプログラ

ムでは、関数 f を用い、アドレスなど I/O 要求のある特定の値にプログラム識別子を埋め込む。ストレージ装置およびネットワーク装置では、逆関数 g によりプログラム識別子が埋め込まれた特定の値から元の値とプログラム識別子を取り出す。これにより、プロトコルを変更せずにプログラム識別子をストレージ装置およびネットワーク装置に渡すことが可能となる。

【0006】

すなわち、本発明の代表的特徴は、上記手段を用いて、プログラムに設定されたプログラム識別子をストレージ装置およびネットワーク装置に渡し、ストレージ装置およびネットワーク装置でアクセス制御を行う。本明細書ではこれをプログラム識別子方式と呼ぶ。

【0007】

プログラム識別子方式では、ストレージ装置およびネットワーク装置の修正が必要となり、その分実現可能性が低くなる。本発明の別の特徴に従えば、ストレージ装置およびネットワーク装置に既に存在するアクセス制御機構を用いる。すなわち、ネットワーク上では計算機およびストレージ装置にネットワークアドレスが割当てられており、計算機およびネットワーク装置およびストレージ装置においてネットワークアドレスによるアクセス制御が可能である。そこで、計算機に対して複数のネットワークアドレスを割当て、計算機においてプログラム識別子とネットワークアドレスを対応付けする。プログラム識別子に対応するネットワークアドレスでストレージ装置と通信し、I/O コマンドを送信する。ストレージ装置およびネットワーク装置では計算機に割当てたネットワークアドレスごとにアクセス可否を設定する。これにより、ストレージ装置およびネットワーク装置においてはネットワークアドレスでアクセス制御を行っているが、計算機ではプログラム識別子に対応したネットワークアドレスを用いているため、実質的に I/O 要求を発行したプログラムによりアクセス制御を行っていることとなる。本明細書ではこれをネットワークアドレス変換方式と呼ぶ。

【0008】

ネットワークアドレス変換方式では、プログラム識別子とネットワークアドレスの対応表が計算機上に存在する。計算機上のユーザ（ルートを含む）からアク

セス可能な場所に保存されていると、計算機が乗っ取られた場合に対応表が不正に書き換えられてしまい、本発明の課題が解決できない。このため、ネットワークアドレス対応表は計算機上のユーザがアクセスできない場所に保存する。

【 0 0 0 9 】

【発明の実施の形態】

以下、本発明の実施形態について説明する。

まず、プログラム識別子を特定の値に埋め込む関数と、該関数によりプログラム識別子が埋め込まれた値から元の値とプログラム識別子を取り出す関数について述べる。以降簡略化のために、「プログラム識別子を特定の値に埋め込む関数」を識別子埋め込み関数 f （関数 f ）、「関数 f によりプログラム識別子が埋め込まれた値から元の値とプログラム識別子を取り出す関数」を識別子取出し関数 g （逆関数 g ）と記述する。関数 f / 逆関数 g は、プログラム識別子のある値に対して埋め込みおよび取り出しが可能であればよい。つまり、関数 f は 2 つの値を入力とし 1 つの値を出力する関数で、逆関数 g は 1 つの値を入力し 2 つの値を出力する関数であり、 z が $f(x, y)$ の出力である場合に $g(z)$ は (x, y) を出力する。最も簡単な例としては、埋め込む値の上位数ビットをプログラム識別子用に割当て、関数 f では該数ビットにプログラム識別子を書き込み、逆関数 g では該数ビットからプログラム識別子を読み込む方式が考えられる。このような関数 f / 逆関数 g は、論理ボリュームの実用量が小さくアドレスの上位ビットを使用しない場合において利用できる。関数 f / 逆関数 g の種類は以降に説明する実施形態に関係ないため、以降の説明では関数 f / 逆関数 g とだけ述べる。

【 0 0 1 0 】

図 1 は関数 f を用いるプログラム 1 0 1 であり、例えばデータベース管理システムや Web サーバなどストレージを使用するミドルウェアやアプリケーションプログラムである。プログラム 1 0 1 は、処理本体 1 0 2 と、該プログラム 1 0 1 のストレージへの入出力を行う I/O 処理部 1 0 3 で構成される。本特許を実現するために、I/O 処理部 1 0 3 には関数 f を用いてアドレスにプログラム識別子を埋め込むアドレス変換部 1 0 4 がある。他に OS に対して I/O 要求を発行する I/O 要求発行部 1 0 5 がある。

【0011】

処理本体102でストレージへの入出力が必要になると、IO処理部103にIO要求が来る。IO処理部103では、まずアドレス変換部103にIO要求を渡す。図2にアドレス変換部103での処理を示す。アドレス変換部103では、まずIO要求が保護論理ボリュームに対するIO要求かを調べる(201)。保護論理ボリュームとは、本発明によりプログラムによるアクセス制御が行われている論理ボリュームのことを指す。保護論理ボリュームに対するIO要求である場合、IO要求にあるアドレスとプログラムに設定されたプログラム識別子関数fの入力に与え識別子付アドレスを生成し、IO要求のアドレスに設定する(202)。保護論理ボリュームに対するIO要求でない場合は、そのまま終了する。アドレス変換部103から出力されたIO要求はIO要求発行部105によりOSに対してIO要求を発行する。

【0012】

実施形態例1を図3に示す。実施形態例1は、ネットワークアドレス変換方式を用いストレージ装置に存在するアクセス制御機能を利用して実現した本発明の計算機システムである。図3の計算機システムは、計算機301とネットワーク装置302とストレージ装置303で構成される。計算機301では、プログラムや計算機資源を管理するOS305が動作しており、OS305の管理の元でプログラム101が動作する。プログラム101は図1で説明したとおりである。すなわちプログラム101は、ストレージへの入出力が必要となり、そのIO要求が保護論理ボリュームに対するIO要求であった場合には、当該プログラムに設定されたプログラム識別子を埋め込んだ識別子付きアドレスに変換してIO要求を発行する。ここで、計算機301やOS305は、特定の計算機およびOSに制限されることはない。ネットワークは、TCP/IP (Transmission Control Protocol/Internet Protocol) ネットワーク、あるいはSAN (Storage Area Network) が好適であり、ネットワーク装置302はそれぞれ種類のネットワーク装置となる。TCP/IPネットワークである場合、ネットワーク装置302はハブやスイッチやルータやゲートウェイとなる。SANである場合、ネットワー

ク装置 302 は FC (Fibre Channel) スイッチとなる。ストレージ装置 303 はネットワークの種類に依存し、TCP/IP ネットワークである場合には NAS (Network Attached Storage) や iSCSI (Internet Small Computer Systems Interface) 対応のディスク装置であり、SAN である場合には RAID (Redundant Array of Independent Disks) 装置などの FC 対応のストレージ装置である。ストレージ装置 303 は、計算機 301 に対して論理ボリューム 311 を提供している。論理ボリュームとはディスク装置が計算機に提供するディスクスペースであり、論理デバイスや論理ユニットと呼ばれるものも論理ボリュームに含む。

【0013】

プログラム 101 は OS 305 に対して IO 要求を発行する。通常、OS では複数のプロセスから発行される IO 要求をバッファリングし、最終的にそれぞれの装置に対応したデバイスドライバ、および基板上のマイクロプログラムにおいて IO コマンドをストレージ装置に発行する。IO コマンド発行部 307 は、デバイスドライバおよびマイクロプログラムなどを示す。本発明では、IO 要求を IO コマンド発行部 307 に渡す前にアドレス逆変換部 306 に渡す。アドレス逆変換部 306 での処理を図 4 に示す。

【0014】

IO 要求が保護論理ボリュームに対する IO 要求かを調べる (401)。保護論理ボリュームに対する IO 要求でない場合は、そのまま終了する。保護論理ボリュームに対する IO 要求である場合には、IO 要求のアドレスを逆関数 g の入力として与え、元のアドレスとプログラム識別子を生成する (402)。続いて、ネットワークアドレス対応表 308 を用い論理ボリューム識別子と生成されたプログラム識別子に対応するネットワークアドレスを検索する (403)。ネットワークアドレス対応表 308 の例を図 5 に示す。ネットワークアドレス対応表 308 は、論理ボリューム識別子とプログラム識別子とネットワークアドレスから構成されている。「*」はそのカラム内で具体的に設定された識別子以外の任意の識別子を表す。図 5 の例では、識別子が 001 であるプログラムからの論理

ボリューム L V 1 への I O 要求は a a a のネットワークアドレスで通信を行い、論理ボリューム L V 2 への I O 要求は b b b のネットワークアドレスで通信を行い、識別子が 0 0 3 であるプログラムからの保護論理ボリュームへの I O 要求は c c c のネットワークアドレスで通信を行うことを表している。さらに、保護論理ボリュームへの I O 要求であるがネットワークアドレス対応表で設定されないパターンのために、論理ボリューム識別子が「*」でプログラム識別子が「*」である項目を必ず作成する。このパターンに該当する I O 要求は必ずアクセス拒否される I O 要求であるため、このパターンのネットワークアドレス（図 5 の例では d d d）では、ストレージ装置 3 0 3 では通信不可となるよう設定する。ネットワークアドレスが得られたら該ネットワークアドレスを計算機のネットワークアドレスとして設定し、逆関数 g から得られた元のアドレスを I O 要求のアドレスに設定し、終了する（4 0 4）。

【0015】

アドレス変換部 3 0 6 から出力された I O 要求は I O コマンド発行部 3 0 7 に渡され、設定された計算機のネットワークアドレスでストレージ装置と通信を行い、I O コマンドを送信する。

【0016】

ストレージ装置 3 0 3 では、接続要求があると通信可否判定部 3 0 9 において接続要求元のアドレスによる通信可否が判定される。ストレージ装置で通信不可と設定されたアドレスで通信した I O コマンドは、ストレージ装置に送信されずにエラーとなる。通信可と設定されたアドレスで通信した I O コマンドは、ストレージ装置に送信され、I O コマンド処理部 3 1 0 に渡り、処理される。

【0017】

実施形態例 1 は計算機 3 0 1 およびネットワーク装置 3 0 2 およびストレージ装置 3 0 3 がそれぞれ 1 台の構成であるが、計算機またはネットワーク装置またはストレージ装置が 1 台以上の計算機システムでもほぼ同じであるため、説明は省略する。

【0018】

実施形態例 2 を図 6 に示す。実施形態例 2 は、ネットワークアドレス変換方式

を用いネットワーク装置に存在するアクセス制御機能を利用して実現した本発明の計算機システムである。計算機 301 の構成、アドレス変換部 306 および I/O コマンド発行部 307 および I/O コマンド処理部 310 の内部の動作は、図 3 の実施形態例 1 と同じである。従って、それぞれ図 3 と同一符号で示す。実施形態例 1 と異なる点は、通信可否判定部 609 がネットワーク装置 602 に存在し、ネットワーク装置 602 にてアクセス制御が行われている点である。

【0019】

実施形態例 1 と同様に、実施形態例 2 も計算機 301 およびネットワーク装置 602 およびストレージ装置 303 がそれぞれ 1 台の構成であるが、計算機またはネットワーク装置またはストレージ装置が 1 台以上の計算機システムでもほぼ同じであるため、説明は省略する。

【0020】

実施形態例 3 を図 7 に示す。実施形態例 3 は、プログラム識別子方式を用いストレージ装置においてアクセス制御を実施した本発明の計算機システムである。計算機システムの構成は、実施形態例 1 と同様のため省略する。

【0021】

プログラム 704 は、プログラム識別子をアドレスに埋め込んだ I/O 要求を発行し、OS 705 が I/O コマンド発行部 706 においてストレージ装置 703 に対して I/O コマンドを発行する。計算機 701 から I/O コマンドを受け取ったストレージ装置 703 は、I/O コマンドに従い論理ボリューム 710 へ I/O を行う I/O コマンド処理部 708 へ渡す前に、アクセス可否判定部 707 へ I/O コマンドを送る。

アクセス可否判定部 707 ではプログラム識別子により I/O コマンドを処理してよいかを判定する。アクセス可否判定部 707 の処理の流れを図 8 に示す。I/O コマンドが保護論理ボリュームに対するものかをチェックする (801)。保護論理ボリュームに対する I/O コマンドでなければ、何もせずに次の I/O コマンド処理部 708 に渡される。保護論理ボリュームに対する I/O コマンドである場合、I/O コマンド内のアドレスを逆関数 g の入力に与え、元のアドレスとプログラム識別子を生成する (802)。論理ボリューム識別子とプログラム識別子を用

いアクセス可否判定表 709 を検索し (803)、アクセスが許可されているかを調べる (804)。図 9 にアクセス可否判定表の例を示す。図 9 の例では、論理ボリューム LV1 にはプログラム識別子 001 と 002 が、論理ボリューム LV2 にはプログラム識別子 001 が、論理ボリューム LV3 にはプログラム識別子 003 が、それぞれ許可されていることを示す。アクセスが許可されている場合、IO コマンド内のアドレスを逆関数 g から生成した元のアドレスに設定し (805)、終了する。アクセスが許可されていない場合は、IO コマンド処理部に IO コマンドを渡さず、エラーを返す (806)。

【0022】

実施形態例 1 と同様に、実施形態例 3 も計算機 701 およびネットワーク装置 702 およびストレージ装置 703 がそれぞれ 1 台の構成であるが、計算機またはネットワーク装置またはストレージ装置が 1 台以上の計算機システムでもほぼ同じであるため、説明は省略する。

【0023】

実施形態例 4 を図 10 に示す。実施形態例 4 は、プログラム識別子方式を用いネットワーク装置においてアクセス制御を実施した本発明の計算機システムである。計算機システムの構成は、実施形態例 1 と同様のため省略する。

プログラム 1004 は、プログラム識別子をアドレスに埋め込んだ IO 要求を発行し、OS 1005 が IO コマンド発行部 1006 においてストレージ装置 1003 に対して IO コマンドを発行する。ネットワーク装置 1002 では、ネットワークを流れるパケットを制御するために、通信可否判定部 1007 を持つ。

【0024】

通信可否判定部 1007 ではパケットを送信先へ転送してよいかを判断する。通信可否判定部 1007 の処理の流れを図 11 に示す。通信可否判定部 1007 では、IO コマンドを運ぶパケットから IO コマンドを抜き出し (1101)、該 IO コマンドが保護論理ボリュームに対する IO コマンドかを調べる (1102)。保護論理ボリュームに対する IO コマンドでなければ、そのままパケットを転送する。保護論理ボリュームに対する IO コマンドであれば、IO コマンド内のアドレスを逆関数 g の入力に与え、元のアドレスとプログラム識別子を生成

する(1103)。ストレージ装置識別子と論理ボリューム識別子とプログラム識別子を用い通信可否判定表1008を検索し(1104)、通信が許可されているかを調べる(1105)。図12に通信可否判定表の例を示す。図12の例では、ストレージ装置識別子ST1のストレージ装置にある論理ボリュームLV1に対してはプログラム識別子001と002が、ストレージ装置識別子ST2のストレージ装置にある論理ボリュームLV1に対してはプログラム識別子001が、ストレージ装置識別子ST2のストレージ装置にある論理ボリュームLV2に対してはプログラム識別子003が、それぞれ許可されていることを示す。通信が許可されている場合、IOコマンド内のアドレスを逆関数gから生成した元のアドレスに設定し(1106)、パケットを転送する。通信が許可されていない場合は、パケットを破棄し、計算機1001にエラーを返す(1107)。

【0025】

実施形態例1と同様に、実施形態例4も計算機1001およびネットワーク装置1002およびストレージ装置1003がそれぞれ1台の構成であるが、計算機またはネットワーク装置またはストレージ装置が1台以上の計算機システムでもほぼ同じであるため、説明は省略する。

【0026】

説明した4つの実施形態例いずれの場合もOS上で動作するプログラムは図1で説明したプログラム101を前提としたが、保護論理ボリュームに対してのIO要求がアドレスにプログラム識別子を埋め込まないIO要求であるプログラムが動作していても問題ない。なぜなら、そのようなプログラムのIO要求が保護論理ボリュームに対して発行された場合、実施形態例1および実施形態例2では、アドレス変換部306およびアドレス変換部406において正しくないプログラム識別子が生成され、アドレス変換表の検索の結果通信不可能なネットワークアドレスが設定され、ネットワーク装置およびストレージ装置において通信不可能とされる。一方、実施形態例3では、アクセス可否判定部707において正しくないプログラム識別子が生成され、アクセス可否判定表でアクセス不可と判定される。実施形態例4では、通信可否判定部1007において正しくないプログラム識別子が生成され、通信可否判定表で通信不可と判定される。

【 0 0 2 7 】

【発明の効果】

本発明を用いることにより、保護論理ボリュームは設定されたプログラム以外からはアクセスすることが出来ない。このため、計算機が不正使用されても直接データをアクセスすることは出来ず、データの盗み見や改竄などを防ぐことが可能となる。

【図面の簡単な説明】

【図 1】

保護論理ボリュームにアクセスするプログラムを示す概念図である。

【図 2】

アドレス変換部 1 0 4 の動作フローを示すフローチャートである。

【図 3】

本発明の一実施形態である計算機システムの機能ブロック図である。

【図 4】

上記実施形態のアドレス逆変換部 3 0 6 の動作フローを示すフローチャートである。

【図 5】

上記実施形態のネットワークアドレス対応表 3 0 8 のデータ構成図である。

【図 6】

本発明の別の実施形態である計算機システムの機能ブロック図である。

【図 7】

本発明の更に別の実施形態である計算機システムの機能ブロック図である。

【図 8】

上記実施形態のアクセス可否判定部 7 0 7 の動作フローを示すフローチャートである。

【図 9】

上記実施形態のアクセス可否判定表 7 0 9 のデータ構成図である。

【図 1 0】

本発明の更に別の実施形態である計算機システムの機能ブロック図である。

【図 1 1】

上記実施形態の通信可否判定部 1 0 0 7 の動作フローを示すフローチャートである。

【図 1 2】

上記実施形態の通信可否判定表 1 0 0 8 のデータ構成図である。

【符号の説明】

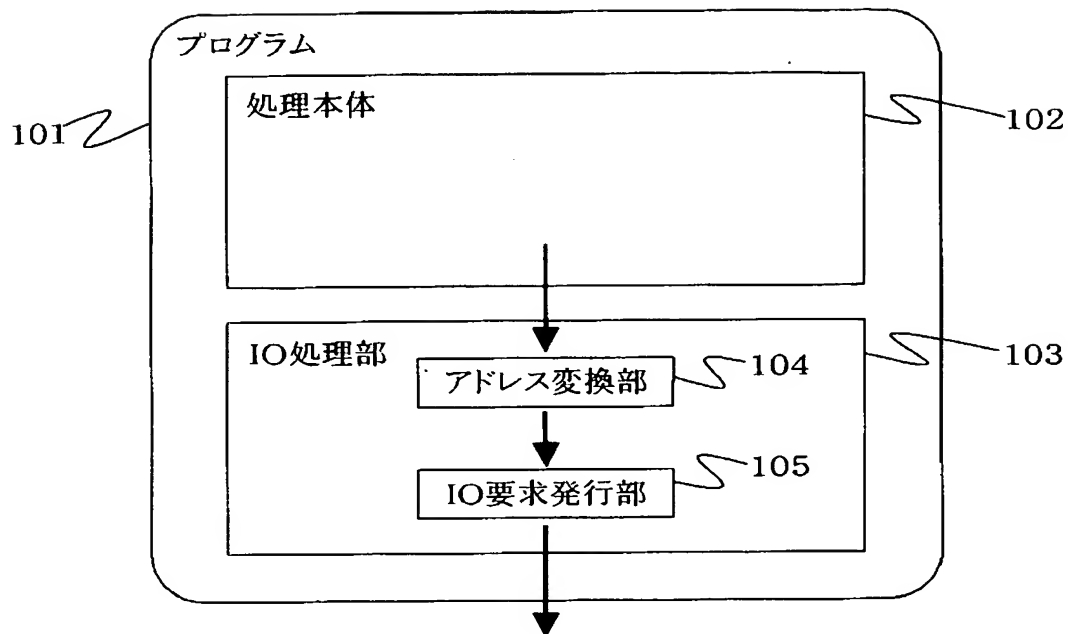
1 0 1、7 0 4、1 0 0 4：プログラム
 3 0 1、7 0 1、1 0 0 1：計算機
 3 0 2、7 0 2、1 0 0 2：ネットワーク装置
 3 0 3、6 0 3、7 0 3、1 0 0 3：ストレージ装置
 3 0 5、7 0 5、1 0 0 5：OS
 3 1 1、7 1 0、1 0 1 0：論理ボリューム
 3 0 8：ネットワークアドレス対応表
 7 0 9：アクセス可否判定表
 1 0 0 8：通信可否判定表。

【書類名】

図面

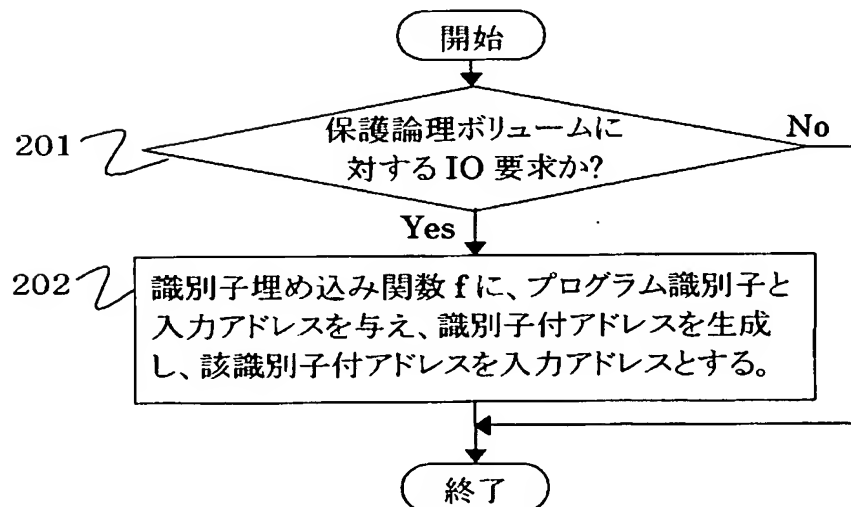
【図 1】

図1



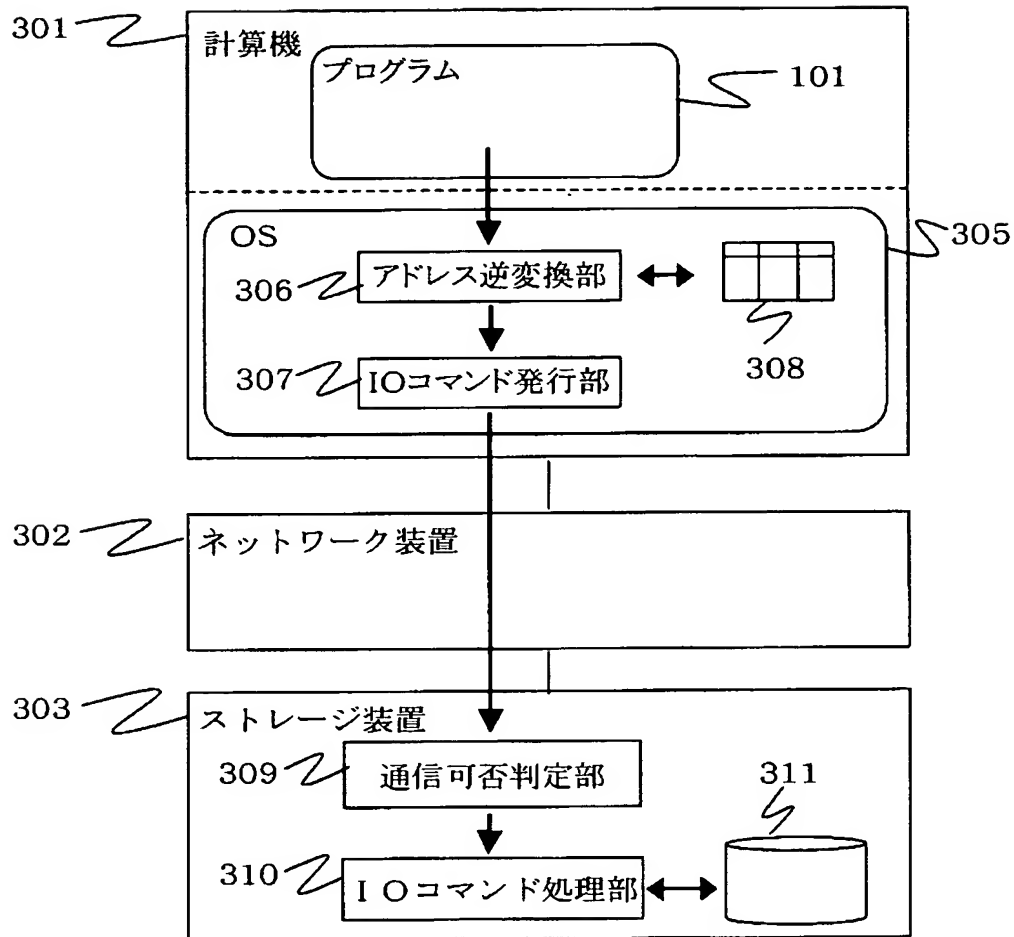
【図 2】

図2

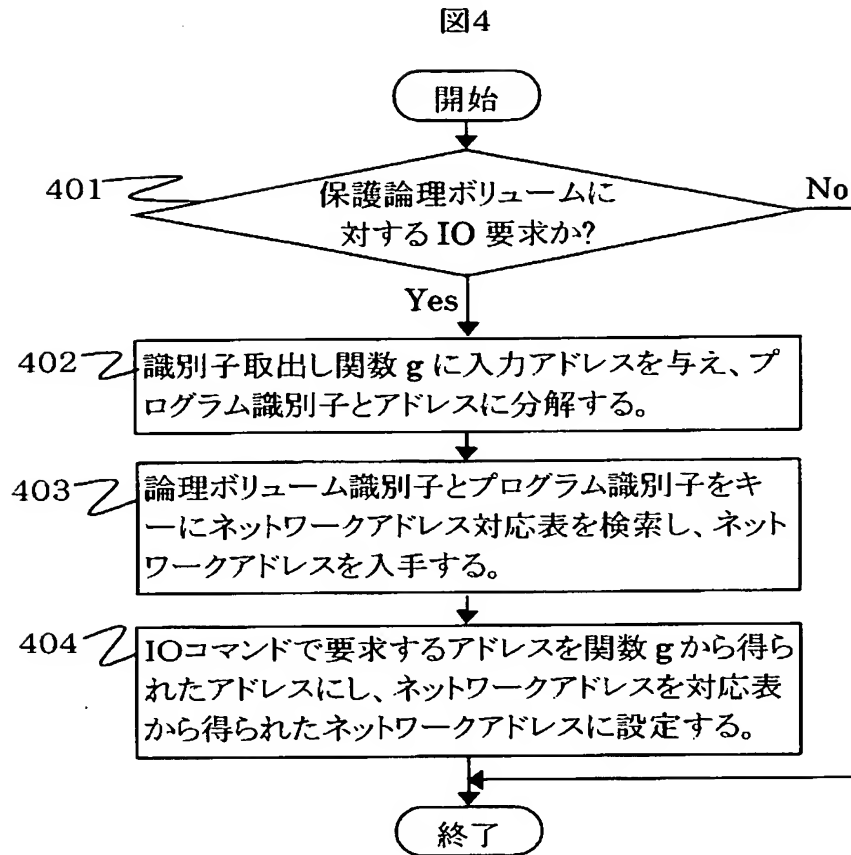


【図 3】

図3



【図 4】



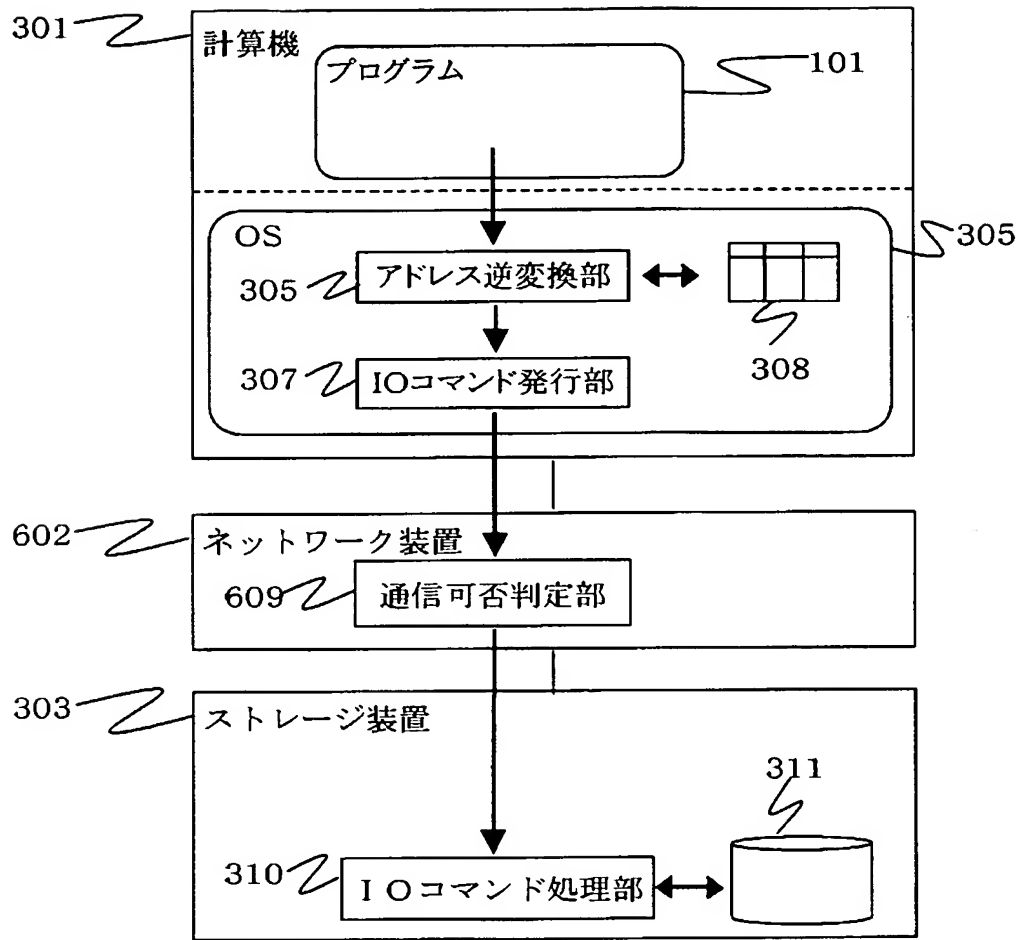
【図 5】

図5

論理ボリューム識別子	プログラム識別子	ネットワークアドレス
LV1	001	aaa
*	002	bbb
LV2	*	ccc
*	*	ddd

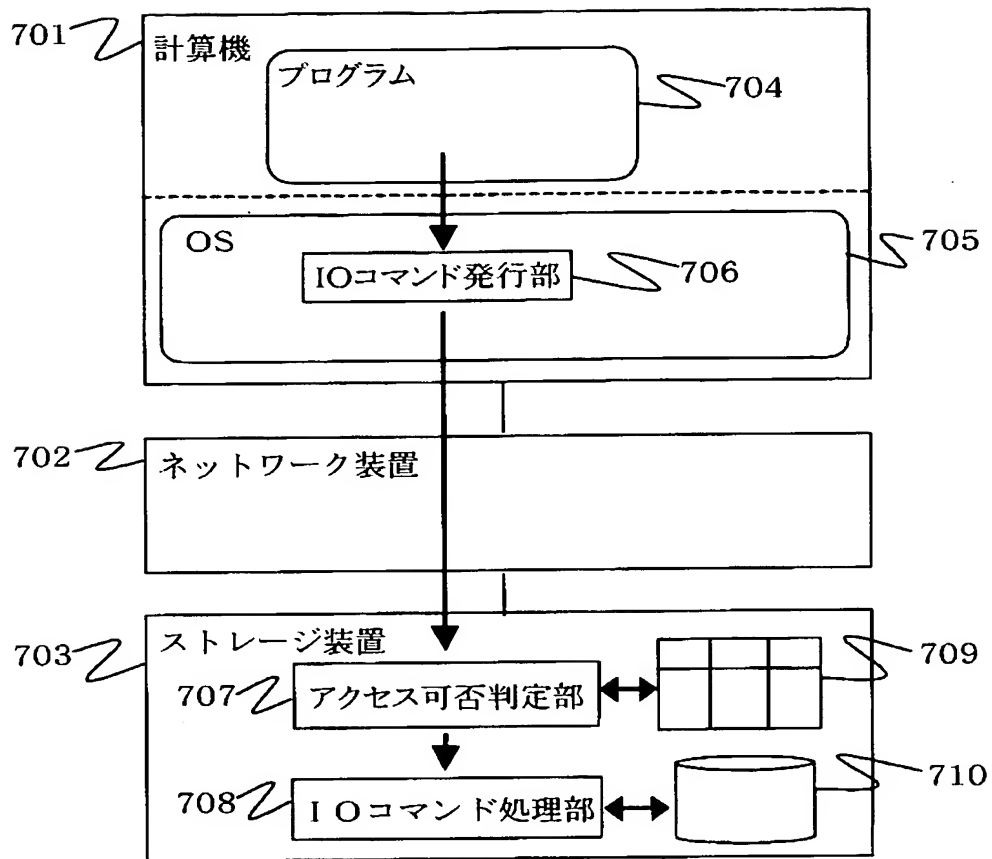
【図 6】

図6

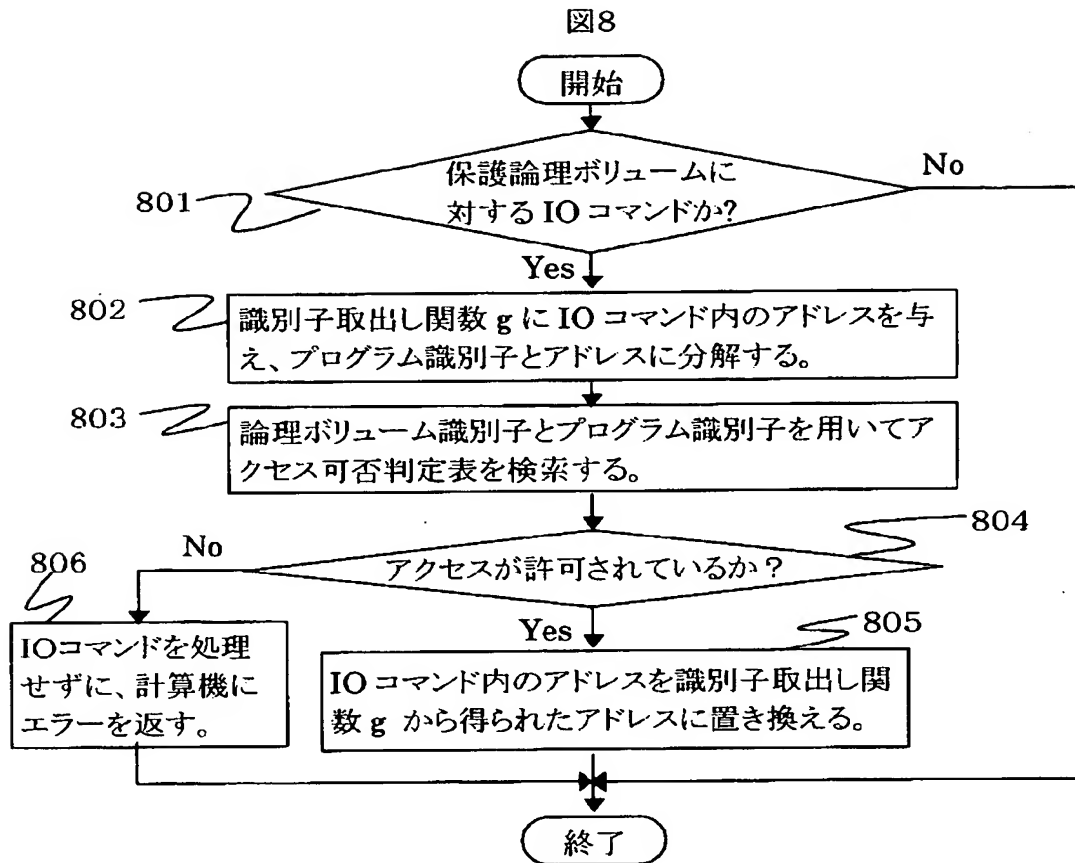


【図 7】

図7



【図 8】



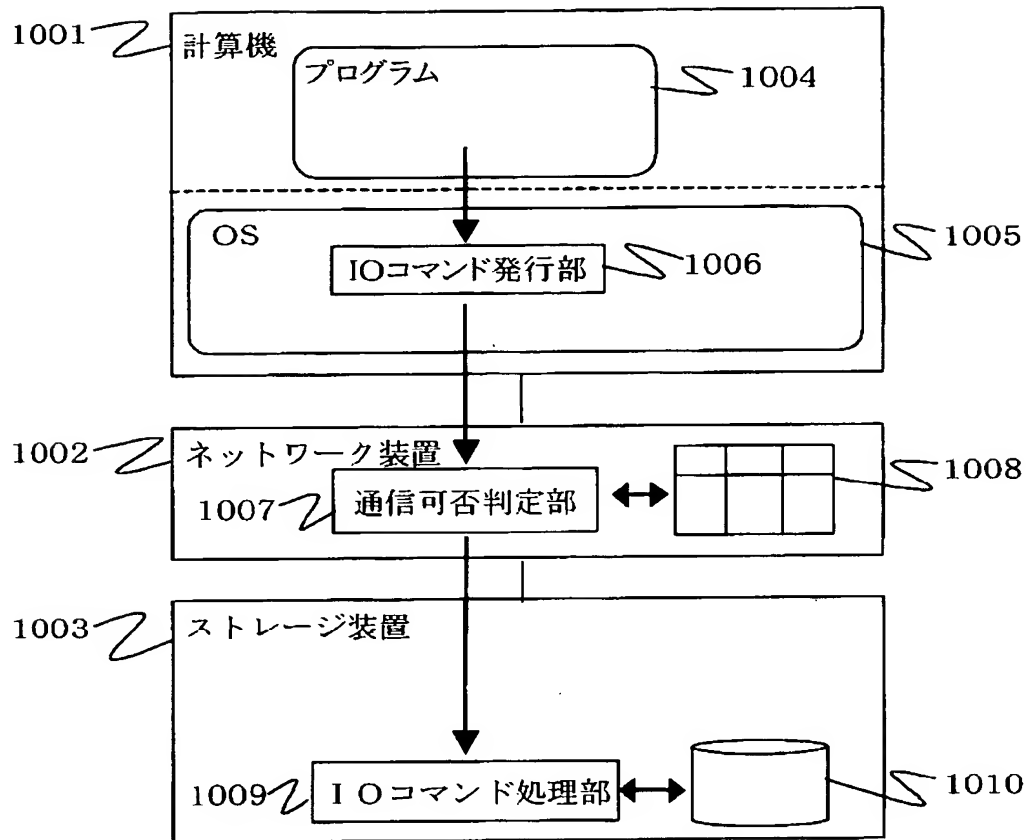
【図 9】

図 9

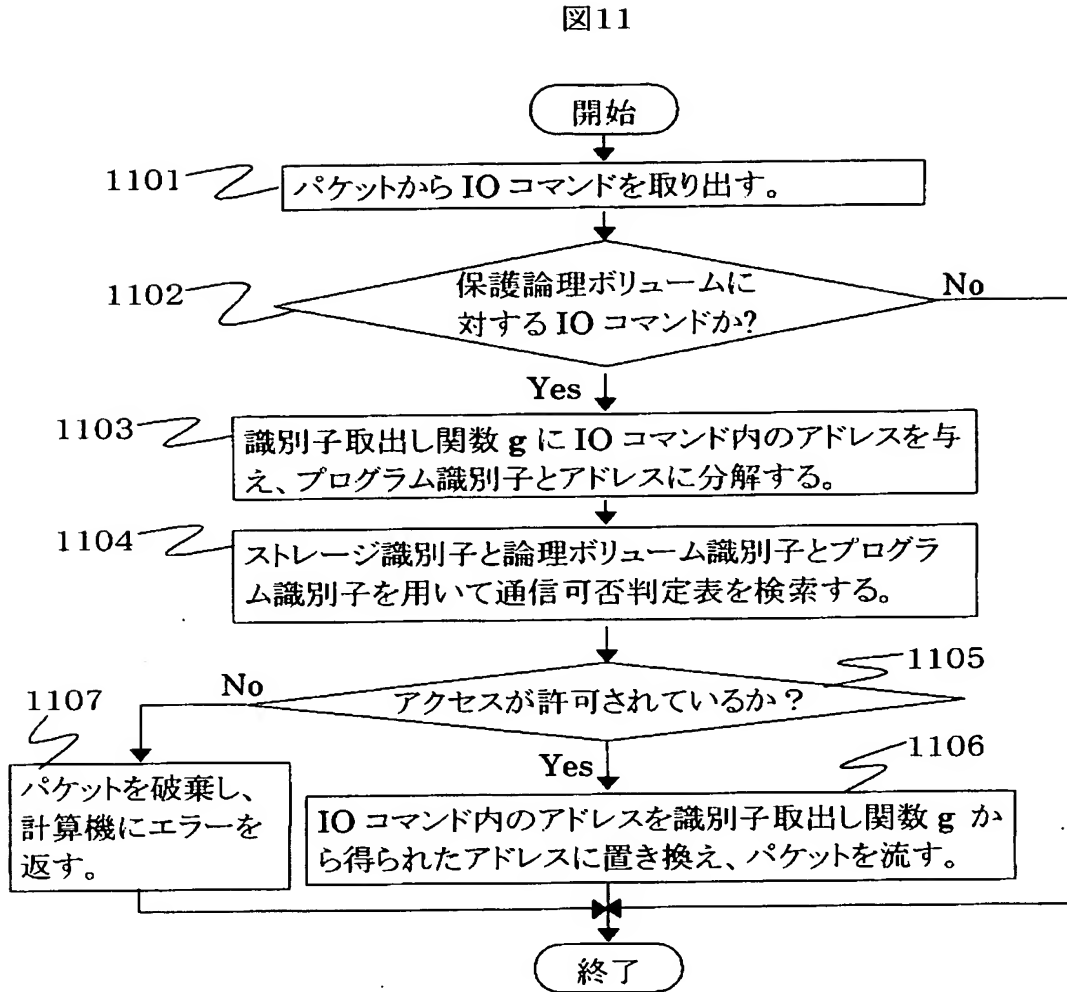
論理ボリューム識別子	プログラム識別子
LV1	001
LV1	002
LV2	001
LV3	003

【図 10】

図10



【図 11】



【図 12】

図12

ストレージ装置識別子	論理ボリューム識別子	プログラム識別子
ST1	LV1	001
ST1	LV1	002
ST2	LV1	001
ST2	LV2	003

【書類名】 要約書

【要約】

【課題】 計算機が不正使用された場合にデータの盗み見や改竄を防ぐ。

【解決手段】 ストレージ装置でアクセス制御が行われていないために、計算機が不正使用された場合にデータの盗み見や改竄が起こってしまう。このため、計算機以外でアクセス制御の仕組みを構築する事で解決する。即ち、ストレージ装置およびネットワーク装置において計算機上で実行しているプログラムを単位としたアクセス制御を行う。実現可能性を高めるため、各種プロトコルの拡張は行わずに実現する。

【効果】 指定されたプログラム以外からはデータをアクセスすることは出来なくなるため、計算機が不正使用されてもデータの盗み見や改竄などを防ぐことが可能となる。

【選択図】 図 3

認定・付加情報

特許出願の番号	特願 2 0 0 3 - 0 9 3 1 4 0
受付番号	5 0 3 0 0 5 2 3 2 3 9
書類名	特許願
担当官	第七担当上席 0 0 9 6
作成日	平成 1 5 年 4 月 1 日

< 認定情報・付加情報 >

【提出日】 平成15年 3月31日

次頁無

特願 2 0 0 3 - 0 9 3 1 4 0

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 1 0 8]

1. 変更年月日	1 9 9 0 年 8 月 3 1 日
[変更理由]	新規登録
住 所	東京都千代田区神田駿河台 4 丁目 6 番地
氏 名	株式会社日立製作所